DOCUMENT RESUME

ED 295 586 IR 013 179

TITLE Telecommunications Policy Research Conference. Computer and Communications Security Section. Papers.
INSTITUTION Telecommunications Policy Research Conference, Inc., Washington, DC.
PUB DATE Sep 87
NOTE 13p.; Paper presented at the Telecommunications Policy Research Conference (15th, Airlie, VA, September 27-30, 1987). For the conference program and additional papers, see IR 013 160-182.
PUB TYPE Viewpoints (120) -- Reports - Descriptive (141) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS Access to Information; *Banking; *Confidentiality; Disclosure; *Federal Government; Federal Regulation; *Information Utilization; Public Policy; *Telecommunications
IDENTIFIERS Computer Security; *Cryptology; *Europe (West); United States

ABSTRACT

In his paper, "European Needs and Attitudes towards Information Security," Richard I. Polis notes that the needs for security in computer systems, telecommunications, and media are rather uniform throughout Western Europe, and are seen as being significantly different from the needs in the United States. Recognition of these needs is, however, quite varied; attitudes towards the best methods for satisfying the needs are even more varied. The situation with respect to those needs and attitudes is described for the major countries of Western Europe, as well as both official and unofficial attitudes towards policy and regulation of information security technology, particularly cryptology. Pointing out that, with a few exceptions, neither official nor unofficial policy level organizations are prepared to follow the position advocated by the U.S. Government in such matters, Polis concludes that the practical impossibility of regulation, coupled with the clear need for large scale deployment of effective, inexpensive cryptology in the private sector, will lead to the decline of the degree of regulation to the vanishing point. (Author/EW)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED295586

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

TELECOMMUNICATIONS POLICY RESEARCH CONFERENCE

Computer and Communications Security Section

Airlie, Virginia

September 27-30, 1987

IR013179

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Edward Zajec

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

Wed 8:15

COMPUTER AND COMMUNICATIONS SECURITY
Chair: Charles Wilk

Richard I. Polis: European Needs and Attitudes Towards Information Security

The needs for security of information (in computer systems, on telecommunications and on media) are rather uniform throughout Western Europe, and are seen as being significantly different from the needs in the United States. Recognition of these needs is, however, quite varied; attitudes towards the best methods for satisfying the needs are even more varied.

The situation with respect to these needs and attitudes is described for the major countries of Western Europe. The official and unofficial attitudes towards policy and regulation of information security technology (particularly cryptology) is also described for these countries. In particular, it is clear that, with a very few exceptions, neither official nor unofficial policy level organizations are prepared to follow the position advocated by the U.S. Government in such matters.

013179

RICHARD POLIS
GROUPE DE MANAGEMENT, GENEVE
GENEVA MANAGEMENT GROUP

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

X This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

EUROPEAN NEEDS AND ATTITUDES
****

TOWARDS

INFORMATION SECURITY
****

Richard I. Polis

Fifteenth Annual

Telecommunications Policy Research Conference

September 27-30, 1987

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
Edward Zajec

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

9, Grand'Rue, case postale 137, CH – 1260 Nyon – Suisse
Téléphone: (022) 61 97 72 – Télex: 419 991

IR013179

GMG

ABSTRACT

The needs for security of information (in computer systems, on telecommunications and on media) are rather uniform throughout Western Europe, and are seen as being significantly different from the needs in the United States. Recognition of these needs is, however, quite varied; attitudes towards the best methods for satifying the needs are even more varied.

The situation with respect to these needs and attitudes is described for the major countries of Western Europe. The official and unofficial attitudes towards policy and regulation of information security technology (particularly cryptology) is also described for these countries. In particular, it is clear that, with a very few exceptions, neither official nor unofficial policy level organizations are prepared to follow the position advocated by the U.S. Government in such matters.

The purpose of this presentation is to try to provide some insight into the European situation concerning needs for and attitudes towards information security. The presentation is made from the perspective of my company, Geneva Management Group, whose principal business is the design of systems for protecting information; our clients are major financial and industrial companies throughout Western Europe.

The major points relate broadly to all forms of information security, but the emphasis is on cryptology; this is because most effective systems for protecting information ultimately depend upon the use of cryptology, and the overall level of protection achieved is therefore a direct function of the strength of the cryptologic algorithm and its associated system of key management.

I will begin by discussing the actual and perceived needs in Europe for information security, with particular emphasis on the level of protection required. Next, I will discuss both official and unofficial attitudes towards what must be protected and how this protection should be achieved. I will assume that this audience is familiar with the U.S. approach to regulation of this technology. It is clear that there is a substantial difference in the basic concept of regulating cryptology between the United States and virtually all European countries; for this reason, it cannot be expected that Europe will follow what appears to be the U.S. trend in this matter.

Finally, I would like to make a few remarks about the inherent necessity of regulating the private use of cryptology. My principal point is that such regulation is neither necessary, nor desirable, nor even possible. There is clear evidence that this fact is increasingly, although not yet universally, recognized in Western Europe. Its major implication is that one cannot expect to force private parties to restrict their use of cryptology to any one or more algorithm created or endorsed by government bodies.

European Needs

There is a strong need, throughout Europe, to protect information stored on various media and/or transiting public telecommunications. This need derives not only from certain legislative requirements for the confidentiality of information (e.g. bank secrecy and data privacy laws), but also from the commer-

./..

cial and political realities affecting both financial and industrial companies; it is particularly important for multinational companies. The entire problem will become even more acute when most restrictions on trans-border operations within the European Economic Community are abolished, as is intended to be the case by 1992.

The degree of protection needed is quite high. Europeans do not particularly need protection against "hackers" or petty criminals. They need protection against organized crime, major corporations and governments. Such opponents are characterized by the presence of serious motivation (and therefore the willingness to expend significant sums to attack a system), access to substantial resources, and the possession or ability to purchase whatever technological expertise is required.

A few examples of actual successful and attempted penetrations of information security in Western Europe are illustrative and instructive.

The first concerns an attack by organized crime against a financial institution with the objective of perpetrating a large scale fraud. In this case, it is estimated that the criminal organization invested the equivalent of US$ 5'000'000 in technical preparations. The criminal gain from a successful fraud of this nature has been estimated at approximately 100 times this investment. One must rely on estimates because the precise identities of the persons responsible remains unknown to this day.

The second example is that of a bank in one country whose customer account data was illicitly obtained by the government of another country. This not only caused severe problems for many customers of that bank, but also resulted in a loss of business due to the bank's visible inability to protect the confidentiality of its customers' affairs. This example illustrates a rather frequent situation: legal operations in one country may be subject to illegal attack and surveillance by another government in its attempt to enforce its laws outside its proper jurisdiction. It is noteworthy that most European bankers are quite familiar with the repeated attempts of the U.S. Government in this regard.

The third example is a multiple case and concerns many of the extractive industries. Certain of their communications are regularly monitored by both private and state-owned competitors. In many cases, such monitoring cannot be legally preven-

./..

ted. The sophistication with which this monitoring is conducted is frequently equivalent to that found in the electronic intelligence operations of the major powers.

In addition to the above, there is a further need that may be considered more or less real. Many European executives are aware of the extent to which certain governments (including the U.S. Government) monitor international (and sometimes domestic) communications. In general, such people have little confidence in the intentions of their own governments, much less foreign governments. There is consequently a need for protection at a level which can defeat these monitoring efforts.

Attitudes Concerning What to Protect

Official attitudes towards what information should be protected are relatively easy to understand, but are also relatively unimportant.

In a few countries, bank secrecy laws mandate the protection of customer information, but most banks have other, more important reasons to safeguard such data. In nearly all European countries, information about individuals must be protected, but there are virtually no real penalites for failure to do so since the emphasis in such legislation is on the identification and registration of data bases containing this type of information.

Technological information is generally not subject to official protection requirements, except where these derive from treaty committments with the U.S.; in such cases, enforcement has little political support and is virtually nil.

In contrast, there is a wide spectrum of non-official attitudes about what data must be protected. These attitudes do not vary significantly from one country to another, but do differ somewhat in different industries and differ markedly from one enterprise to another.

In general, the financial industry is most aware of the need for serious protection. They see the need to protect both customer data and transactions.

Customer data must be protected because the European banking customer expects his affairs to be private; failure to pro-

./..

tect this privacy can cause a loss of confidence in the bank. Transactions must be protected because of the demonstrable fraud losses occurring when such protection is not adequate.

Certain industrial concerns also see an important need for protecting information. In their case, the information is typically related either to markets or to the details of proprietary technology. Protecting such information is needed to maintain their competitive advantage. In this respect, it should be noted that many of these companies operate in competition with state-owned enterprises, sometimes within their home countries; they are consequently interested in protecting this information from various governments, including their own.

Attitudes on How to Protect

Attitudes on how to achieve the required level and types of protection are even more varied. This must be discussed in at least three separate categories, which can be called non-official, semi-official and official, according to the degree of government involvement.

On the purely non-official level, one finds the various enterprises with some need for information security. The attitudes among these enterprises span the complete spectrum, from those who seek only a "cosmetic" level of security to those who require a level equal to that of the best military equipment.

Today, a significant (though declining) proportion of enterprises merely wish to be seen to take some action to protect their information. Such companies are interested in what might be called "cosmetic" security. They typically either do not install any cryptologic protection at all, or install cryptology based on some publicly available algorithm such as DES of RSA. Since they are not interested in real protection, they are indifferent to any controversy over the quality of these algorithms. As an aside, they are also indifferent to any issues of operating performance, since operational difficulties are merely seen as on acceptable excuse for restricting the extent to which cryptology is applied.

In contrast, a growing number of enterprises want real protection. Such institutions require cryptology that is both operationally convenient and highly secure. They increasingly

./..

turn towards the idea of a proprietary solution, which is created expressly for the given enterprise. Moreover, since a very large proportion of companies in this group wish to be protected against governments, they are totally uninterested in any solution that is promoted by any official body.

The proprietary, company-specific approach is clearly the trend in Europe. There have already been several successes with proprietary cryptology; several more systems, including some which will have very high visibility, are in development. The trend to proprietary cryptology can be expected to increase dramatically as these successes in developing company-specific information security mechanisms and proprietary cryptologic algorithms becomes better known.

The semi-official level is principally concerned with the activities of various standardization bodies. The semi-official situation has undergone considerable change in the past year.

Prior to that time, there was considerable pressure to standardize cryptology in Europe. This pressure resulted from an alliance of various manufacturers (who prefer not to be involved in customer-specific work) and various end-users who sought an endorsement of the more cosmetic approaches. However, such standardization attempts have always been controversial.

The controversy had two principal sources. The first was the continuing debate over the quality of the potential candidates for a standard algorithm, chiefly DES and RSA. The second was a growing realization that standardizing cryptology weakens security, regardless of the merits of the algorithm involved. This last point, which has always been well understood by professional cryptologists, was clearly explained to the appropriate ISO working group by the commanding general of the British GCHQ (roughly their equivalent of NSA).

Partly as a result of the above, the following events have recently occurred: (1) ISO has officially decided not to standardize any cryptologic algorithm; (2) CCITT has formally stated that no CCITT recommendation will include a particular cryptologic algorithm now or in the future. In addition, several country and industry standardization organizations have simply abandoned all discussion of standardized cryptology.

In Europe, standardized cryptology is a dead issue.

./..

The official level is also quite different from its counterpart in the U.S. There has never been any serious official attempt to standardize cryptology in any country of Western Europe, but there are various attempts to officially regulate the use of cryptology by private parties. These vary widely from one country to another.

At one extreme are the countries (e.g. Switzerland, Sweden) in which there is no statutory authority whatsoever for the regulation of cryptology. Anyone may import, export and install any type of cryptologic device, and may use this to encrypt any form of information, including information passing over public telecommunications and by wireless transmission. This is increasingly the trend. In fact, it would be surprising if the new generation (digital) of cellular mobile telephone systems did not routinely provide cryptologic interfaces in the subscriber equipment.

In most countries of Europe, there is still some regulation of cryptology, but the degree of regulation is necessarily declining. Even when the use of private cryptology over common carrier facilities is nominally prohibited, exceptions to this prohibition are increasingly easy to obtain. Moreover, these exceptions are frequently obtained for the installation of high quality equipment on such a large scale that monitoring the purposes for which this equipment is used becomes impossible.

The regulators are more and more in the position of King Canute. They can order the tide to stop, but they will still get wet.

Necessity for Regulation

Today, regulation of the private use of cryptology is neither necessary nor desirable; moreover, it is impossible.

To see why this regulation is not necessary, let us consider the main potential objectives of such regulation. There are only two: (1) to deny hostile parties within a country the ability to have secret communications and (2) to insure that private parties with a legitimate need for protection have access to sound means of protection. Unfortunately, there is an obvious conflict between these two unless one makes the totally unreasonable assumption that the cryptologic design capability within government is superior to all cryptologic

./..

expertise outside of government. The unreasonable nature of this assumption is generally recognized in Europe.

In any case, regulation cannot deny the ability to hostile parties to construct cryptologic mechanisms; it can only provide a means of attack in the courts when such parties are apprehended. Clearly, such parties will typically be guilty of far more serious offenses.

Regulation is also not necessary to insure the availability of good cryptology. There are several companies in existence which can supply cryptology of virtually any desired strength; they can do this in a way which permits a positive, unambiguous demonstration of this strength, with the possibility of submitting the demonstration to an independent expertise.

Regulation of cryptology is not desirable. The increasing dependence of society on sophisticated computer systems accessed via telecommunications requires that cryptologic protection be encouraged and deployed on a large scale. Regulating the nature and extent of cryptology can only serve to maintain the vulnerabilities of such systems.

For example, in France today approximately 250'000 individuals and enterprises regularly employ home banking services; this number is expected to increase dramatically in the future. Steps are therefore being taken to place a sophisticated cryptologic device in the hands of each home banking customer. By 1992, it is entirely possible that several million such devices will be in the hands of customers throughout Europe. Each of these devices will provide a level of cryptologic protection that is at least equal to the best military cryptologic equipment deployed today, and each device has a unit production cost of approximately $ 30.

The above is an illustration of why regulation of private cryptology today is impossible. One no longer needs expensive manufacturing, large scale computers or custom integrated circuits to develop secure, high performance cryptology. In many cases, strong cryptology can be implemented using ordinary microprocessors, less powerful than those used in personal computers. In fact cryptologic algorithms can readily be implemented in software.

The public literature dealing with cryptology is now sufficiently comprehensive that it is not difficult to understand how to make a strong algorithm if one is not concerned about

./..

efficient performance in large scale applications. Even then, there are several companies that can supply algorithms, equipment or both. Equipment production can also be arranged to take place within the country of intended use, thus eliminating considerations of import and export controls; even design can be arranged to take place in an appropriate country.

Finally, any authority which attempts to mandate the nature of cryptology used within its jurisdiction must be prepared to indemnify users against loss resulting from a penetration. It is clear that no European government agency is prepared to do this. In fact, most European telecommunications Administrations are not even willing to address the subject of encryption for fear that doing so might imply a performance warranty for some particular algorithm or equipment.

This practical impossibility of regulation, coupled with the clear need for large scale deployment of effective, inexpensive cryptology in the private sector leads therefore to the conclusion that the degree of regulation will inexorably decline to the vanishing point. The trend is clear in Europe; it should become equally clear in the U.S.